Document Control No. GCCS.2.1.SAM-1 April 1996

April 24, 1996

Global Command and Control System (GCCS)
System Administrator Manual
HP-UX 9.0.7

Version 2.1

Prepared by:

Inter-National Research Institute (INRI)
12200 Sunrise Valley Drive, Suite 300
Reston, Virginia 22091

Table of Contents

Name of Document

The following conventions have been used in this document:

Helvetica Font	Used to indicate screen options to be selected. For example, select either the Yes or the No button.
[Helvetica Font]	Used to indicate keys to be pressed. For example, press [ESC].
`Courier Font`	Used to indicate an entry to be typed at the keyboard, UNIX commands, and screen text. For example, type `get/etc/resolv.conf`.
"Quotation Marks"	Used to indicate prompts and messages that appear on the screen.
Italics	Used for emphasis.

THIS PAGE INTENTIONALLY LEFT BLANK

Section One

Scope

The Global Command and Control System (GCCS) is an Automated Information System (AIS) supporting the Department of Defense (DoD). GCCS produces, integrates, and fields new hardware and software components designed to provide the Joint Planning and Execution Community (JPEC) with new technology and functionality. GCCS system integration emphasizes use of the commercial off-the-shelf (COTS) products and merges the capabilities of a modern local area network (LAN), a UNIX-based client/server architecture, a desktop-style Graphical User Interface (GUI), and a Relational Database Management System (RDBMS).

GCCS is intended to help joint operation planners satisfy their deliberate and crisis planning responsibilities via access to a useful, user-tested, integrated set of analytical tools and via flexible data transfer capabilities. The GCCS client/server architecture provides a firm foundation for linking external systems and GCCS components, permitting easy access to applications and faster, more reliable data transfers within a secure environment. At the heart of GCCS is a large database and application server connected to a LAN. The GCCS LAN interconnects the GCCS server with a variety of workstations (DOS and Microsoft Windows PCs, Macintosh, UNIX, and other X-Windows clients) that run associated software and application packages. The GCCS LAN will also connect with wide area networks (WANs) supporting a standard LAN design.

The GCCS concept is designed to support a wide range of mission applications through a diverse set of application "segments" executed under a Common Operating Environment (COE). All segments that pass Defense Information Systems Agency (DISA) integration testing become part of the GCCS baseline. The Government executive agent that provides the segment is responsible for testing and validating the functionality of the segment. The scope of GCCS Version 2.1 is to implement the functionality required for the shutdown of the current Honeywell-based Worldwide Military Command and Control System (WWMCCS). GCCS Version 2.1 contains the GCCS core functionality required for the shutdown of WWMCCS, as well as other critical legacy applications from earlier versions of GCCS. The emphasis of the GCCS Version 2.1 installation is the implementation of this core functionality.

GCCS can be installed on Hewlett Packard (HP) TAC-3s and TAC-4s independently from the Solaris GCCS; however, dependencies can be established between the HP and Solaris. Current Solaris installations establish an Executive Manager Server (EMSERVER) workstation. Facilities are provided on the HP and Solaris software that will allow a single Solaris EMSERVER to act as the entry point for building and configuring user accounts. If the site has established an EMSERVER, the HP installation should be configured to use that server. If the site only has HP workstations, a single HP can be established as the EMSERVER. This System Administrator Manual assumes each site will establish a Solaris EMSERVER.

Many of the GCCS applications require access to a Database Server (DBSERVER). If a DBSERVER is not available at the site, many of these applications will not run.

The GCCS architecture is specifically designed with flexibility and COTS standardization to allow interconnection with new networks and systems as they are deployed. This architecture will easily adapt to and assimilate new applications and functions.

GCCS is designed with the user in mind. GCCS is flexible, yet fully functional, which necessitates a complex

system design, with a regular and effective technical "behind the scenes" System Administration (SA) activity. Consequently, trained SA personnel are essential to the satisfactory operation of the GCCS resources at each site. This System Administrator Manual provides technical SA guidance for DoD sites receiving GCCS Version 2.1.

This System Administrator Manual provides configuration guidance specific to the GCCS Version 2.1 for the HP series workstations. These procedures do not address system administration tasks and procedures that apply to SunOS machines. Those procedures are covered in detail in the *GCCS 2.1 System Administration Manual*.

This document is divided into the following sections:

Section 2

Domain Name Server

2.1 Overview

Currently, three popular methods are used to translate or resolve host names into IP addresses in GCCS: (1) Host tables, (2) Network Information Service (NIS) and (3) Domain Name Service (DNS).

Host tables are located on each system on the network in the `/etc` directory. This requires maintenance of each table separately, which can be an administrative burden on all but the smallest of networks.

When using NIS, a single host file, found under `/h/EM/nis_files/host` in the NIS or NIS+ server, is used by all GCCS platforms. This file should not be used to resolve names of platforms outside the site's LAN. See Section 3, *Network Information Service Administration for more information on NIS*.

DNS is the service, by which hosts are able to connect to other hosts on the SIPRNET without knowing each hosts IP address. Each site usually maintains a DNS server that connects to other DNS servers in an attempt to resolve host names to Internet Protocol (IP) addresses across the SIPRNET. If a DNS server has been established at your site, an HP DNS server is not required; instead, you should point your `/etc/resolv.conf` file to that name server. It is extremely important that your site’s DNS server contain an entry for your HP workstation or the HP will not initialize networking functions.

DNS is an application layer protocol that is part of the standard Transmission Control Protocol/Internet Protocol (TCP/IP) suite. DNS is in essence a naming service: it obtains and provides information about hosts on a network. DNS performs naming between hosts within the local administrative domain and across domain boundaries. It is distributed among a set of servers, commonly known as "name servers," each of which implements DNS by running a daemon called `named`.

One fundamental difference between Solaris and HP is the use of the `nsswitch.conf` file. One purpose of the `nsswitch.conf` file is to provide system-level alternatives to the local system files that may be available in served files (either NIS or DNS). The GCCS HP 9.07 Operating System does not support a service similar to the `nsswitch.conf` file. Since the HP Operating System does not offer a choice after DNS hostname resolution such as referring to the local `/etc/hosts` file, the configuration of the DNS server is extremely important.

Every network device attached to a TCP/IP network is identified by a unique 32-bit IP address. Any device that has an IP address can be assigned a host name. While host names are not required, they make it easier for the user to use the network and may be used interchangeably with a system's IP address.

2.2 Defining Domain Nameservers

The `/etc/resolv.conf` file defines the name servers for a domain. This file should be set up as follows:

STEP 1: Type the following command:

```
vi /etc/resolv.conf
```

STEP 2: Type `i` [RETURN].

STEP 3: Type the following commands:

`domain` [TAB] [`yourdomain.smil.mil`] [RETURN]

(where `yourdomain.smil.mil` is your domain name)

`nameserver` [TAB] [`ip_address_of_primary_name_server`] [RETURN]

(where `ip_address_of_primary_name_server` is the address of the primary name server)

`nameserver` [TAB] [`ip_address_of_secondary_name_server`] [RETURN]

(where `ip_address_of_secondary_name_server` is the address of the secondary name server)

`nameserver` [TAB] [`ip_address_of_offsite_backup_name_server`] [ESC]

(where `ip_address_of_offsite_backup_name_server` is the address of the offsite backup server)

`:wq!`

NOTE: When defining the name servers for a domain, ensure that commands do not contain any extra lines or spaces. If commands contain extra spaces or lines, the resolver will not work and will not provide an error message.

The `/etc/resolv.conf` file provides a pathway to a name server for devices in a domain that are not name servers. A maximum of three name servers may be listed in the `/etc/resolv.conf` file.

2.3 Setting Up a Name Server

Follow the steps below to set up a name server:

STEP 1: Create the `/etc/resolv.conf` file by typing the following command:

`domain` [TAB] [`yourdomain.gcc.smil.mil`] [RETURN]

(where `yourdomain.gcc.smil.mil` is your domain name)

STEP 2: Create the command file `/etc/hosts_to_named` by typing the following command:

```
vi named.cmd
```

Type `i` to edit the following:

`-d [your.domain]` [RETURN] (specify your domain name)

`-n [170.200.4]` [RETURN] (specify your IP address)

`-H [hosts]` [RETURN] (specify the source of name-to-IP information)

`-r` [RETURN] (if this nameserver is a “root server”)

`:wq!` [RETURN]

STEP 3: Execute `/etc/hosts_to_named` to create the DNS maps by typing the following command:

```
# hosts_to_named -f named.cmd
```

The following text will appear on your screen. The text may vary according to site.

```
Translating hosts to lower case ...

Collecting network data ...

170.200.4

15.13.164

Creating list of multi-homed hosts ...

Creating "A" data (name to address mapping) for net
xxx.xxx.x ...

Creating "PTR" data (address to name mapping) for net
xxx.xxx.x...

Creating "A" data (name to address mapping) for net
xx.xx.xxx ...

Creating "PTR" data (address to name mapping) for net
xx.xx.xxx ...

Creating "MX" (mail exchanger) data ...

Building default named.boot file ...

done
```

STEP 4: View the `named.boot` file created by `hosts_to_named` by typing the following command:

```
# more named.boot
```

The following text will appear on your screen. The text may vary according to site.

```
;
; type domain source file
;
directory /etc ; running directory for named
primary     0.0.127.IN-ADDR.ARPA    db.127.0.0
primary     vancouver.center        db.vancouver
primary     4.200.170.IN-ADDR.ARPA  db.170.200.4
primary     164.13.15.IN-ADDR.ARPA  db.15.13.164
cache .     db.cache
#
```

STEP 5: Examine the “maps” created as a result of the above command. Type the following command:

```
ls -al
```

The following text will appear on your screen. The text may vary according to site.

```
ls -al db*
-rw-rw-rw- 1 root sys         251 Apr 9 09:54 db.127.0.0
-rw-rw-rw- 1 root sys         255 Apr 9 10:03 db.15.13.164
-rw-rw-rw- 1 root sys         335 Apr 9 09:54 db.170.200.4
-rw-rw-rw- 1 root sys         134 Apr 9 09:54 db.cache
-rw-rw-rw- 1 root sys         629 Apr 9 10:03 db.vancouver
#
```

STEP 6: Verify that `/etc/named` is an executable; `/etc/netbsdsrc` will start `named` upon initialization.

STEP 7: Type: `ls -al /etc/named`. The files listed should be preceded with `-rwx r-x r-x`.

STEP 8: Start `/etc/named` manually by typing `/etc/named`.

STEP 9: Verify DNS functionality by typing the following command:

`nslookup` [`hostname`]

(where `hostname` is your hostname)

The following text will appear on your screen. The text may vary according to site.

Name Server: `nameserver.site.smil.mil`

Address: `xxx.xxx.xxx.xxx`

Name: `hostname.gcc.smil.mil`

Address: `xxx.xxx.xxx.xxx`

STEP 10: The machine nameserver is now a name server for the domain `site.smil.mil.` Other DNS capable hosts (e.g., HP-UX) can refer to this nameserver by creating a `/etc/resolv.conf` file containing:

```
search [site.smil.mil]
```

(where `smil.mil` is your domain name)

```
nameserver xxx.xxx.xxx.xxx
```

(where `x` represents the IP address of the `nameserver`).

2.4 Debugging Hints

Below are items that may assist the System Administrator in troubleshooting DNS problems.

- Check the `/usr/adm/messages` file if the `in.named` daemon does not start. Error messages are printed to `/usr/adm/messages` if syslog is turned on.
- Check the cache by signaling the `in.named` daemon by executing the following command:

  ```
  kill -INT `cat /etc/named.pid` [RETURN]
  ```

  This will cause a dump to the `/var/tmp/named_dump.db` file.
- The `nslookup` facility provides insight into how DNS sees the network. Enter the command

  ```
  nslookup
  ```

  and use the help option to get a list of available options.

2.5 Updating the Name Server

When updating the name server, always edit files on the primary name server and make sure you increment the serial number.

Type the following command to signal the `in.named` daemon of the change:

```
kill -HUP `cat /etc/named.pid`[RETURN]
```

This command will insert the Process ID (PID) of the named daemon as an argument for the kill command (`HUP` is the UNIX signal name for "Hangup"):

Use the following command to force an update of the secondary name server:

```
usr/bin/in.named -xfer -z jdef.disa.smil.mil -f db.hosts -s 0
backfire.jdef.disa.smil.mil [RETURN]
```

(where: `z =` the zone

`f =` the database to update

`s =` the serial number on the secondary server is the same as the # on the primary server)

If the above command does not work, perform the following steps on the secondary name server. The steps will force an update.

STEP 1: Kill the `in.named` daemon.

STEP 2: Remove the `db.hosts` and `db.rev.hosts` from the secondary name server.

STEP 3: Touch the `db.hosts` and `db.rev.hosts` files.

STEP 4: Restart the daemon.

Section 3

Network Information Service Administration

3.1 Overview of NIS

Given the architectural differences between the HP and Solaris Operating Systems, many system functions that operate on the Sparc workstations do not operate the same on HP workstations. The most important differences are the Network Information Services (NIS) and the `/etc/nsswitch.conf` file. GCCS uses NIS+ under Solaris, which is a version of NIS that has been enhanced over the previous NIS or yellow pages. The GCCS HP Operating System currently supports yellow pages. Since GCCS has chosen not to serve all of the system files by the Solaris NIS+ server and therefore has chosen not to operate in an NIS compatibility mode, a separate NIS server needs to be established on an HP workstation.

NIS is generally required for GCCS Version 2.1, but the decision to implement NIS is strictly based on site requirements. Host name resolution for GCCS is provided by DNS, and user validation and authentication services can be handled through the `/etc/passwd, /etc/shadow`, and `/etc/group` files.

The current implementation of the NIS software for the HP does not support the passing of passwords from the Solaris NIS+ system to the HP. Therefore, if a user changes his or her password on the Solaris system, he or she will need to make the same change on the HP system, and vice versa.

NIS provides the capability to maintain a centralized database of information and make it available to all systems attached to the LAN. For GCCS, this information includes user names, group account information, and the host names of systems.

3.1.1 NIS Namespace

The arrangement of information stored by NIS is known as the "NIS namespace." Although the namespace can be arranged in a variety of ways to suit a specific organization, all sites use the same structural components: directories, tables, and groups. These components are called NIS objects. NIS objects can be arranged into a hierarchy that resembles a UNIX filesystem. However, the following differences exist:

- € Although UNIX and NIS both use directories, the other objects in an NIS namespace are tables and groups, not files.
- € The NIS namespace is administered only through NIS administration commands designed for that purpose; it cannot be administered with standard UNIX filesystem commands.
- € NIS directories are designed to hold other directories, tables, and groups. NIS directories are normally arranged in configurations called "domains," which are designed to support separate portions of the namespace.

The NIS domain is supported by an NIS server, which stores the domain's directories, groups, and tables. The NIS server answers requests for access from users, administrators, and applications. A NIS client is a workstation that has been set up to receive NIS service. Setting up an NIS client consists of making the client a member of the proper NIS groups, verifying its home domain, and running its NIS initialization utility.

3.1.2 NIS Tables

NIS stores information in 16 preconfigured tables that approximate files contained in the UNIX `/etc` directory. The tables are:

€ Host	€ Bootparams	€ Passwd	€ Cred
€ Group	€ Netgroup	€ Mail_Aliases	€ Timezone
€ Networks	€ Netmasks	€ Eithers	€ Services
€ Protocols	€ RPC	€ Auto_Home	€ Auto_Master

GCCS Version 2.1 uses only three of these tables: `Host`, `Passwd`, and `Group`. These tables are different from UNIX files because they have a column and entry (row) structure that stores data that can be accessed in multiple ways. These tables cannot be accessed by standard UNIX commands, but rather with a suite of NIS commands, most beginning with `yp`, that allow access to information contained within the NIS tables.

3.1.3 NIS Security

The security features of NIS are provided by two means: authorization and authentication. Authorization is the process by which a server identifies the access rights granted to a principal. The principal refers to the user or client workstation. Authentication is the process by which an NIS server identifies the NIS principal that sent a particular request. Authentication is the most significant portion of the process used by GCCS. Authentication is the means by which an NIS server verifies the "credentials" of an NIS principal.

3.1.4 Executive Manager Interaction with NIS

The GCCS Executive Manager (EM) is the primary interface with NIS. The EM’s Security Manager creates groups, users, and passwords and then formats the result in a form required to input data into the NIS tables. The EM's Security Manager also stores the results in files located in `/h/EM/nis_files`. The EM uses the NIS command `ypmake` to update the NIS tables using those files.

3.2 Configuring NIS

3.2.1 NIS Servers

Listed below are facts regarding NIS servers that the System Administrator should keep in mind.

- € Master and Client are the two kinds of NIS Servers.
- € The `ypserv` command must always be run.
- € A Master server is required.
- € All maintenance MUST be done on the NIS Master Server.
- € "Source" files for NIS are found on the NIS Master Server.
- € At least one NIS Server must exist per IP subnet.

€ 3.2.1.1 Configuring the /etc/passwd and /etc/group Files

NIS uses a + entry at the end of the local data files to tell the system to refer to the NIS maps if the desired entry is not in the local files. This only applies to the `passwd` and `group` maps.

Adding a "+" entry after the local entries in `/etc/passwd` and `/etc/group` will use the NIS tablespace for user and group resolution.

NOTE: Do not put an asterisk "*" in the password field, the system will not refer to the NIS maps if the desired entry is not in the local files. HP-UX assumes an "*" represents an invalid `/etc/passwd` file entry and ignores the command.

3.2.1.2 Configuring the Master NIS Server

The following procedures will initialize an NIS master server. These procedures are normally performed during the installation process in the execution of the `/h/EM/systools/EM_install` script. Follow the steps below to re-initialize an NIS server.

STEP 1: Execute `/usr/etc/yp/ypinit -m DOM ="[domain.name]" PWFILE=/h/EM/nis_files/passwd`

(where `domain.name` is the NIS domain name).

STEP 2: Execute the command `domainname [domain.name]`

(where `domain.name` is the name of your NIS domain).

STEP 3: Initialize the NIS client services on the Master server by executing the following `/etc/ypbind` command.

STEP 4: Point the Master server to itself by executing `/usr/etc/yp/ypset xxx.xxx.xxx.xxx`

(where `xxx.xxx.xxx.xxx` is the IP address of the NIS Master machine).

STEP 5: Ensure the NIS maps are present and bound to the NIS Master by executing `ypwhich -m`. This will print the NIS Master server name along with a list of NIS maps and the name of the Master server for each map.

STEP 6: Edit the `/etc/netnfsrc` file on the NIS Master machine such that

`NIS_CLIENT=1` appears on the NIS Master machine.

`NIS_MASTER_SERVER=1` appears on the NIS Master machine.

`NISDOMAIN="[your_NIS_domain.gcc]"` appears.

NOTE: Quotation marks are needed in case special characters (e.g. a period) appear in the domainname.

These changes will be implemented the next time the machine is booted.

3.2.1.3 Configuring Slave NIS Server(s)

Follow the steps below to configure Slave NIS Server(s).

STEP 1: Execute `/usr/etc/yp/ypinit -s xxx.xxx.xxx.xxx DOM="domain.name"`

(where `xxx.xxx.xxx.xxx` is the IP address of the Master NIS server and `domain.name` is the NIS domain name).

The NIS Slave server will download its copy of the NIS maps from the Master Server.

STEP 2: Execute the command `domainname domain.name`

(where `domain.name` is the name of your NIS domain).

STEP 3: Initialize the NIS client services on the Master server by executing the following `/etc/ypbind` command.

STEP 4: Point the Master server to itself by executing `/usr/etc/yp/ypset xxx.xxx.xxx.xxx`

(where `xxx.xxx.xxx.xxx` is the IP address of the NIS Slave machine).

STEP 5: Ensure the machine is bound to the NIS server by executing `ypwhich -m`. This will print the NIS Master server name along with a list of NIS maps and the name of the Master server for each map.

STEP 6: Edit the `/etc/netnfsrc` file on the NIS Master machine such that

`NIS_CLIENT=1` appears on the NIS Master machine.

`NIS_SLAVE_SERVER=1` appears on NIS Master slave machines.

`NISDOMAIN= "[your_NIS_domain]"` appears.

(where `your_NIS_domain` is your NIS domain name)

NOTE: Quotation marks are needed in case special characters (e.g., a period) appear in the domainname.

These changes will be implemented the next time the machine is booted.

3.2.1.4 Configuring the NIS Client

€ Add a "+" entry after the local entries in `/etc/passwd` and `/etc/group` to use the NIS tablespace for user and group resolution.

NOTE: Do not put an asterik “*” in the password field or you will NOT "escape" to NIS. HP-UX assumes an "*" represents an invalid `/etc/passwd` file entry and ignores the command.

€ Edit the `/etc/netnfsrc` file on the NIS Client machines such that

NIS_CLIENT=1 appears on NIS Client machine.

NISDOMAIN="`your_NIS_domain`" appears.

NOTE: Quotation marks are needed in case special characters (e.g., a period) appear in the domainname.

These changes will be implemented the next time the machine is booted.

3.2.2 Commonly Used NIS Tools

Listed below is a brief description of commonly used NIS tools and commands.

Tool	Description
`ypcat mapname`	Executes a "cat" on an NIS map. For example, `ypcat hosts` dumps the hosts map to the screen.
`ypcat -k ypservers`	Dumps the list of NIS Servers to the screen.
`ypmatch -k key mapname`	Matches a single NIS map entry. For example, `ypcat -k user passwd` dumps the user’s entry in the passwd map.
`ypwhich`	Displays the server to which host is bound.
`ypwhich -m`	Displays the server to which host is bound and the NIS maps that come from which NIS Master.
`/usr/etc/yp/ypset`	Binds the host to a specific NIS server.
`/usr/etc/yp/ypinit`	Initializes an NIS server.
`/usr/etc/yp/ypmake`	Builds or rebuilds NIS maps.
`yppasswd`	Changes an NIS password.
`yppush`	Manually pushes updated maps to the Slave from the Master.

3.3 NIS Troubleshooting

This section provides assistance in troubleshooting common NIS errors.

3.3.1 NIS Server Problems

A common problem with the NIS Server is when the server is missing information or not being updated. This happens when files are updated on the Master, `ypmake` is run to build the maps and to push them out to the slaves, and one or more slaves does not see the updates.

One possible cause to the problem is when new slave NIS servers have been added without being entered in the NIS Master server. This condition can be confirmed by typing the command:

```
: ypcat -k ypservers
```

This command will dump the NIS Master servers' database of the NIS servers. Use the following steps to add or delete NIS servers.

NOTE: The following steps must be performed on the NIS Master server.

STEP 1: Type `cd /usr/etc/yp/"domain.name"`

(where `domain.name` is the name of the NIS domain).

STEP 2: Type `../makedbm -u ypservers > /tmp/slist` to unpack the `ypservers` map into an ASCII file named `/tmp/slist`.

STEP 3: Edit the file `/tmp/slist` to add or delete any NIS servers. Note that the master is listed twice.

STEP 4: Type `../makedbm /tmp/slist ypservers` to recompile the `dbm` file.

STEP 5: Type `../yppush -v ypservers` to push the `ypservers` map to all of the slaves.

STEP 6: Type `ypcat -k ypservers` or rerun `ypinit` on the NIS Master.

STEP 7: Type `/usr/etc/yp/ypinit -m DOM="nis.domain" PWFILE=/etc/passwd`. This will require reentry of all the NIS Slave servers.

A second possible cause is that `ypmake` has been run on one or more slave servers (all updates should be done only on the Master Server). This problem does not occur as often, and it is more difficult to detect. It is caused by updating the NIS files on the slave, and then running `ypmake` on the slave, which causes the order number of one or more NIS maps to become greater than the order number of that map on the master. Order numbers (date/time map build) can be found by typing

```
/usr/etc/yppoll -h xxx.xxx.xxx.xxx mapname
```

(where `xxx.xxx.xxx.xxx` is the IP address of the NIS server).

NOTE: `yppoll` needs the exact mapname, not the nickname (e.g. `hosts.byaddr` and `hosts.byname`, not `hosts`).

If the NIS slave, not receiving updates, is in the `ypservers` map (`ypcat -k ypservers`), reinitialize the slave by rerunning `ypinit`. To do this, type the following command:

```
/usr/etc/yp/ypinit -s xxx.xxx.xxx.xxx DOM="nis.domain"
```

(where `xxx.xxx.xxx.xxx` is the IP address of the NIS server and `nis.domain` is the name of the NIS domain).

This will purge the existing NIS maps on the slave and download new copies from the NIS master.

3.3.2 Re-establishing the NIS Server

The HP NIS Server is normally established during the installation process in the EM_install script. If it is necessary to re-establish the NIS server, follow the steps below:

STEP 1: Log in as `root` and remove any old NIS setup files by typing

```
cd /usr/etc/yp/previous_nis_domain
rm -rf *
```

STEP 2: Kill the processes `/usr/etc/yp/rpc.yppasswdd, ypserv,` and `ypbind`, if they are running, by typing

```
ps -ef | grep yp
```

Note the PID for `rpc.yppasswdd`, `ypserv`, and `ypbind`. Type

`kill -9 PID` (where `PID` is the process id for `rpc.yppasswdd`).

`kill -9 PID` (where `PID` is the process id for `ypserv`).

`kill -9 PID` (where `PID` is the process id for `ypbind`).

STEP 3: Update the files for NIS located under the `/h/EM/nis_files` directory. Make any necessary updates to the NIS source files. In particular, look at the following:

`hosts`	Enter the IP addresses and host names of all systems that are part of the NIS environment on the LAN. Syntax for this file is the same as `/etc/hosts`. Do not put any aliases in this file.
`passwd`	Make sure `secman` is the only user when installing on a new system for the first time.
`group`	Ensure `gccs` and `admin` groups are defined.

STEP 4: Change the group ID on all the files to `101` and change `owner` to `root`.

STEP 5: Make sure the owner and group files have read/write permission by typing

```
chmod 664 passwd group hosts
```

STEP 6: Start and configure the NIS server by typing

```
ypinit -d nis.domainname
```

STEP 7: Populate the NIS tables from files by typing

```
ypmake DIR=/h/EM/nis_files -d nis.domainname
```

STEP 8: Reboot the machine.

3.4 Changing the User Password From the Root Account

No facility exists to propagate password changes between NIS (HP) and NIS+ (Solaris). Passwords must be changed manually on HP clients. Log in as `root` to the NIS server and type the following command:

```
yppasswd username
```

Prompts will appear instructing you how to change the password.

3.5 Populating the NIS Database From the NIS+ Database

Follow the steps below to populate the NIS database from the NIS+ database.

STEP 1: Log in as `sysadmin` on the NIS+ server.

STEP 2: Open an xterm window.

STEP 3: Type the following command: `niscat passwd.org dir >/tmp/passwd.`

STEP 4: Edit the file:

a. Type `vi /tmp/passwd`.

b. Type `/` (slash).

c. Type `csh` to move to the first instance of `csh`.

d. Type `C` to change to the end of the line.

e. Type `csh` and press [ESC] to change the rest of the line (being edited) to `csh`. Then delete the rest of the line.

f. Type `n` to move to the next instance of `csh`.

g. Type `.` (period) to repeat the last command.

h. Repeat STEPS f and g until all of the extra text after `/bin/csh` for each user is deleted.

i. Type `wq!` when the end of the file is reached.

STEP 5: Type the following command: `niscat group.org dir > /tmp/group`.

STEP 6: Transfer the files via FTP from the EM server to the NIS server.

a. Type `ftp_HP_NIS_server_name`.

b. Type `bin`.

c. Type `send /tmp/passwd /h/EM/nis files/passwd`.

d. Type `send /tmp/group /h/EM/nis files/group`.

e. Type `quit`.

STEP 7: Log out of the EM server.

STEP 8: Log in to the HP NIS server as `sysadmin`.

STEP 9: Initiate an xterm window.

STEP 10: Execute the following command:

```
/usr/etc/yp/ypmake DIR=/h/EM/nis files passwd.
```

STEP 11: Execute the following command:

```
/usr/etc/yp/ypmake DIR=/h/EM/nis files group.
```

STEP 12: Change the `/etc/netnfsrc` file to reflect the new location of the NIS files.

a. Type `vi /etc/netnfsrc`.

b. Type `/` (slash).

c. Type `rpc.yppasswd`.

d. Type `dd`.

e. Type `i`.

f. Type `/usr/etc/yp/rpc.yppasswd /h/EM/nis_files/passwd -m passwd DIR=/h/EM/nis_files.`

g. Press [ESC].

STEP 13: Type `:wq!` and press [RETURN].

THIS PAGE INTENTIONALLY LEFT BLANK

Section 4

Printer Administration

4.1 Scope

Most of the printer administration functions are available through the system administration login. The Printer Admin icon, located on the GCCS desktop, provides the capability to add, delete, and update printers on the system.

4.2 GCCS Desktop Printer Concept of Operations

The purpose of this section is to describe the printing capabilities provided by the GCCS Version 2.1 Session Manager (also known as the "desktop"). Network Printing Support is one of the printing capabilities.

4.2.1 Network Printing Support

Network Printing Support allows users to send output to printers on their GCCS network regardless of the type of workstation, print server hardware, and printer hardware (within the limitations of the hardware identified as supported by the GCCS COE.)

Network Printing Support consists of support to the System Administrator for printer installation and management, and support to the user for printer selection. System Administrators and users will receive support for print queue management through GUIs. System Administration printer support will exist as a distinct GCCS application called Printer Administrator. User print management will be integrated into the GCCS desktop via the User Print Manager function.

g. 4.2.1.1 Printer Administrator

The Printer Administrator function will provide System Administrators the capability to easily manage the functions associated with adding and deleting printers on the GCCS network. The following functions are provided through the printer administrator user interface:

- € Install a connected printer on its attached print server.
- € Make a newly installed printer visible to all print clients on the network.
- € Remove an installed printer from its attached print server and all print clients on the network.

Additional functions provided that relate to the management of printer assets on the GCCS network include the following:

- Query the current available printer list and update the client during system reboot.
- Modify printer characteristics such as description and location.

Queue management functions are similar to functions provided to regular users. Except, System Administrators are allowed to perform queue management functions across the network and manage jobs they did not initiate. The following queue management tasks are supported:

- Remove any print job from any print queue.
- Move a print job from one print queue to another.
- Start or stop an active print queue.

4.2.1.2 User Print Manager

The User Print Manager function enables the user to select the optimal printer for a given print job. The GUI will display a list of available printers that include such details as printer name, print server name, location, description, printer type, and current status. Current status will show how many jobs are currently waiting to be printed on that printer. From this display, the user will select the printer to be used for a given print task. The user will also be able to delete print jobs that have been initiated from an active print queue.

4.3 Configuring HP-UX

Follow the steps below to manually install a printer. HP's System Administrator Manager (SAM) can also perform additional printer administration functions.

STEP 1: Log in to the print client as root.

STEP 2: Enter the following commands:

```
# /usr/lib/lpshut [RETURN]
```

```
# /usr/lib/lpadmin -p[LOCALNAME] -m[PRINTMODEL] / -v/dev/null -
orm[PRINTSERVER] -orp[PRINTERNAME] -ob3 [RETURN]
```

(where `LOCALNAME` is the name the printer that will be called by the system.

`PRINTMODEL` is the type of printer.

`PRINTSERVER` is the host name of the print server.

`PRINTERNAME` is the name of the printer on the remote print server).

```
# /usr/lib/accept [LOCALNAME] [RETURN]
```

(where LOCALNAME is the name the printer that will be called by the system).

/usr/bin/enable [LOCALNAME] [RETURN]

(where LOCALNAME is the name the printer that will be called by the system).

/usr/lib/lpsched [RETURN]

To invoke the HP's SAM follow the steps below:

STEP 1: Log in as `root`.

STEP 2: Type `sam` at the command prompt.

STEP 3: Select Printers/Plotters Administration from the System Administrator Manager window.

STEP 4: Select Printers/Plotters from the Printers/Plotter window.

The local and remote configured printers will appear in the Printers/Plotter Manager window.

Under the Actions pull-down menu, the user can add, delete, and update printers.

29

THIS PAGE INTENTIONALLY LEFT BLANK

Section 5

Disk Administration

HP workstations often come with more than one hard drive. The root disk is normally configured using the `/dev/dsk/c201d6s0` device. HP does not support the partitioning of disks; therefore the entire disk is mounted as `/` (`root`). After the initial disk has been loaded, additional disks need to be configured. The disk configuration steps are performed through an interface developed by HP known as SAM. Follow the steps below to configure additional disks.

5.1 Adding Additional Disks

Follow the steps below to configure additional disks on your system:

STEP 1: Log in as `sysadmin`.

STEP 2: Open an X-terminal window.

STEP 3: Type `xhost +.`

STEP 4: Type `su - root.`

STEP 5: Type your root password at the password prompt.

STEP 6: Type `sam.`

STEP 7: Select Disks and File Systems, then select Open from the System Administrator Manager window.

STEP 8: Select CD ROM, Floppy, and Hard Disks from the list, then select Open from the Disk and File Systems window.

The Disk and File System Manager window will appear listing all of the hard disks and CD ROM drives available to your system.

STEP 9: Highlight an unconfigured disk. Select Add a Hard Disk Drive from the Actions pulldown menu.

STEP 10: Click on Set Disk Usage and Options from the Add a Hard Disk Drive (hostname) window.

STEP 11: Select File System and Swap from the Set Hard Disk Usage and Options window.

STEP 12: Type in the mount point of the hard disk drive in the mount point field. Use `/home2` as the first mount point. If you have additional disks to add after this disk, use `/home1, /home3`, and so forth for your mount points.

STEP 13: Click the Create New File System button. An additional list will appear displaying the

available options for disk size and swap size.

STEP 14: Select the desired amount of swap space. Generally, the total amount of swap space a system should have is approximately two times the amount of workstation RAM, evenly divided between files systems. An additional swap space of approximately 100 Mb should be sufficient.

STEP 15: Click on OK. If the disk has been previously mounted, the following prompt will appear:

```
The disk you have selected has an unmounted file system on it.
By choosing to create a new filesystem on this disk you will
destroy the old file system. Do you want to proceed and create
a new file system?
```

STEP 16: Select OK. The system will display an hour glass until the newfs has been completed. When the system returns to the disk listing, you may either configure additional hard drives or exit SAM.

5.2 Removing Disks and Additional Software

Follow the steps below to remove disks and additional software:

STEP 1: Log in as `sysadmin`.

STEP 2: Select Configure Disks from the Hardware menu.

The resulting window will show the disks on the system and whether they are mounted.

STEP 3: Select the disk to be unmounted.

STEP 4: Select the Unmount button.

THIS PAGE INTENTIONALLY LEFT BLANK